STONESOFT

TCO Whitepaper

Achieving Network Nirvana

How to Reduce Costs and Complexities
While Optimizing Security and Performance

Table of Contents

Executive Summary

In 2009, the network security landscape is expected to undergo a major overhaul and not just because of the economy. According to Nemertes Research, organizations are bucking the fragmented approach to network security of trying to manage a mix of best-of-breed products.* Not only is this type of infrastructure increasingly difficult to manage from a strategic and technical perspective, it is also extremely costly.

With hundreds of security products in the market – ranging from firewall/VPN appliances to load balancers – a typical organization is dealing with, on average, as many as 15 different security products within their infrastructure. That's 15 different products that may need to be implemented, managed and maintained across a geographically dispersed network. As a result, organizations may be dealing with hundreds of security devices that don't necessarily work well together that increase potential points of failure. In fact, industry analyst firm Gartner reports that more than 99 percent of firewall breaches are caused by misconfigurations – not firewall flaws.** That's not a training issue, that's a complexity issue. This problem is further exasperated as IT organizations are asked to reduce resources while increasing service levels to their constituencies.

In short, IT leaders are faced with formidable goals in 2009's tough economic climate – they must look for ways to reduce complexities and costs, while further optimizing network security and performance to meet expanding organizational demands.

Since 2001, Stonesoft has been an innovator in the network security market with a proven track record of simplifying the management of even the most complex networks. Prior to 2001, Stonesoft successfully maintained its position as market leader with its patented StoneBeat high availability technologies for other firewall vendors. With the StoneBeat technology at its foundation, Stonesoft has built the award-winning StoneGate Platform, which unifies firewall, VPN, IPS and SSL VPN, blending integrated threat management, end-to-end high availability and network optimization, into a proactive centrally controlled system. By using the StoneGate Platform, forward-thinking organizations are proactively supporting security best practices, realizing significant operational efficiencies, while dramatically reducing their total cost of ownership (TCO). In fact, the StoneGate solutions typically save organizations as much as 30-70 percent in measureable costs compared to other leading products on the market.

*Nemertes Research Market Analysis Report, July 2008
** *Gartner, Inc., Q&A: Is It More Secure to Use Firewalls from Two Different Vendors, August, 2008*

Based on feedback and actual analysis of organizations that have switched to StoneGate solutions from competitors' products, this whitepaper will help IT leaders understand how they can gain significant savings in the following areas:

- **Administration Cost Savings:** By simplifying the administration of policy and rules management, hardware and software updates, incident management and troubleshooting, as well as reporting and compliance management

- **Hardware & Infrastructure Cost Savings:** By eliminating the need for Multi-protocol Label Switching (MPLS), Border Gateway Protocol (BGP) routers, standby systems and load balancers

- **Communication Cost Savings:** By eliminating the communications costs associated with MPLS, Frame Relay and BGP connections

Administration Cost Savings

Traditionally, selecting best-of-breed network security products from different vendors has been a common practice for most IT organizations that rely on a layered approach to security. Not only has this approach created complex, redundant infrastructures that are extremely labor intensive to maintain, it opens the doors to human error and security threats. Most best-of-breed products have been designed as device-centric appliances with little regard for integration across a layered infrastructure. In addition, when it comes to managing policies and rules, updating configurations and devices, incident management and troubleshooting, this approach has created a siloed approach to managing security and availability.

Greater efficiency through better design has been Stonesoft's quest since the beginning. As part of the company's goal to simplify network management, Stonesoft is the only vendor that provides proactive control with one true centralized command center for real-time management of the most complex networks. This centralized command center – called the StoneGate Management Center – manages the entire StoneGate Platform including its integrated firewall/VPN, IPS and SSL VPN solutions for both physical and virtual environments, as well as third-party device events.

While a lot of vendors claim to have centralized management, Stonesoft has taken the next step by delivering a level of proactive centralized control that is unmatched in the industry. Organizations need to take a close look at the approach vendors use in their fundamental architecture. Is it a bolt-on approach or a built-in fully integrated approach? With the StoneGate Management Center, organizations gain the following built-in capabilities to proactively gain control of network security and performance:

- **Third-party Event Management:** The StoneGate Management Center provides the first platform for proactive network security management of entire networks, including physical and virtual environments, as well as third-party device events. This gives organizations access to real-time device monitoring, event correlation, logging and reporting of the switches, routers and security appliances from different vendors across their networks. As a result, administrators can significantly streamline troubleshooting and incident management time.

- **One-step Management:** Allows organizations to proactively manage hundreds of devices as easily as one – from simple device updates to immediately responding to security threats – from a single console. Security policies and rules can be defined once and automatically pushed to all devices, thereby eliminating costly misconfiguration errors and dramatically decreasing threat response times.

- **Accelerated Incident Management:** Delivers one common, correlated view of physical and virtual networks, as well as third-party events, combined with a powerful data mining engine to significantly reduce the time for troubleshooting, incident investigation and resolution. In addition, administrators can capture historical incident records to more proactively manage network security.

- **Central Repository:** Enables "create once, deploy everywhere" configurations since all components share a common element database. The results are easy component re-use, less administration and fewer human errors. The central repository stores all configuration information for fast recovery, provides customizable role-based access for multiple administrators, and enables the creation of end-customer domains for managing different customer environments with a single management server.

- **Real-time Monitoring & Alerting:** Provides the most comprehensive real-time dashboards of network activity compared to other systems that offer a crude snapshot of events at best. Using easy-to-interpret graphical views, geographic pinpointing of IP addresses, customized alert policies and drill-down and filtering capabilities, organizations can quickly address anomalies and attacks. In addition, a Web portal gives administrators and MSSPs' end customers the ability to monitor network security anytime, anywhere and from any device.

- **Interactive Reporting & Compliance Tools**: Includes easy-to-use, customizable graphical report designs, automated report generation and distribution, comparative analysis of security policies, as well as system auditing and audit trails to significantly streamline the entire process of ensuring regulatory compliance.

The benefits of proactive control within the network security infrastructure of an organization cannot be underestimated. Using this approach, Stonesoft customers report significant reductions in administration costs. Based on extensive research within the Stonesoft community, we have established some cost assumptions as outlined below. On average, Stonesoft customers report that a single full-time equivalent (FTE) or administrator can manage as many as 35-40 devices at any given time. Management of these devices includes:

- Policy and rules management
- Hardware and software updates
- Incident management and troubleshooting
- Reporting and compliance management

As outlined in Example 1, Stonesoft can provide administrative cost savings of as much as 65 percent compared to competitors.

Example 1:

Cost Assumptions

	Stonesoft	Check Point	MSSP	Cisco
No. of Devices/FTE	35-40	15-17	15	10-12
Annual FTE Cost	$120,000	$120,000	NA	$120,000
Annual Cost/Device	$3,428	$8,000	$9,600	$10,900

Annual Costs for a 70-Device Implementation

	Stonesoft	Check Point	MSSP	Cisco
No. of Devices/FTE	35	15	15	11
Annual FTE Cost	$120,000	$120,000	NA	$120,000
No. of Administrators	2	4	NA	6
Annual Cost/Device	$3,428	8,000	9,600	10,900
Total Annual Cost	**$240,000**	**$480,000**	**$672,000**	**$720,000**

4-Year Cost Comparison

	Stonesoft	Check Point	MSSP	Cisco
Year 1	$240,000	$480,000	$672,000	$720,000
Year 2	$240,000	$480,000	$672,000	$720,000
Year 3	$240,000	$480,000	$672,000	$720.000
Year 4	$240,000	$480,000	$672,000	$720,000
Total	**$960,000**	**$1,920,000**	**$2,668.000**	**$2,880,000**

Hardware & Infrastructure Cost Savings

In the realm of network security – or, for that matter, all technology – there have typically been two approaches to solution development. One is to provide an all-inclusive, integrated solution or "built-in" approach, while the other approach requires the purchase of additional "bolt on" products.

From the beginning, Stonesoft's vision has been to simplify network security. That's why the company provides its patented always-on technologies built-in throughout its integrated solutions – firewall/VPN, IPS and SSL VPN – compared to other vendors that require the purchase of additional bolt-on products to try to achieve the same level of connectivity.

Today, the StoneGate Platform includes the following built-in technologies that not only ensure that even the most complex networks are available 24x7, but also make sure they are optimized to support changing organizational demands. The significant benefits provided by these technologies are a direct result of the company's early market-leading StoneBeat technology.

- **Multi-Link™ Communication:** Eliminates network links as single points of failure, by providing seamless VPN failover across multiple circuits. Regardless of the type of connections needed – DSL, leased lines, cable modems and even satellite – Multi-Link can load balance an unlimited number of circuits through a single appliance to ensure always-on network connectivity, superior active/active performance, and optimization for VoIP and other emerging technologies. When multiple circuits are required for redundancy, Multi-Link also eliminates the cost and administration of BGP routers.

- **Drop-in Active Clustering:** Enables the unique clustering of up to 16 devices so organizations are assured the highest availability and scalability from the core to the edge of their networks without the need for expensive standby systems. With drop-in technology, clusters can be easily added into existing infrastructures without complex configuration requirements. When a three-node cluster is configured with a Multi-Link dual circuit, a Five Nines nearly fault-tolerant network can be achieved.

- **Dynamic Server Load Balancing:** Distributes traffic between servers to balance the load efficiently and ensure that services are available when needed. User connections can be intelligently redistributed across server pools based on server availability. When configured with a two-node or three-node firewall cluster, maintenance can be done as needed during business hours with no down time.

- **IPS Serial Inline Clustering:** Ensures that IPS systems protecting internal systems never go down. With the unique "daisy chain" configuration built in to the StoneGate IPS, organizations can be assured that if one IPS sensor should fail, the other IPS sensors in the link will automatically take over and monitor the traffic to keep the information flowing securely. With each IPS added to the cluster, throughput performance increases significantly to ensure scalability for expanding organizations.

- **StoneGate Management Center High Availability:** Enables up to four standby management centers and real-time replication of repository data in the event of downtime so network monitoring never stops.

- **SSL VPN Gateway Redundancy:** Provides clustering of two SSL VPN appliances to form a mirrored access-point pair to ensure that even remote mobile connections never go down.

- **Mobile (IPsec) VPN Gateway Redundancy:** Provides clustering of multiple links to ensure mobile VPN connections are continuously available.

Since these always-on connectivity technologies are built-in, the need to purchase perimeter-based load balancers is eliminated approximately 60-80 percent of the time. In addition, when dealing with remote locations, Stonesoft's technologies include router capabilities at the perimeter, usually eliminating the costs for a routing device or gateway.

Communication Cost Savings

MPLS vs. ISP

The cost of circuits for connecting organizations has dropped dramatically over the last few years. The migration from Frame Relay circuits to MPLS and other offerings have helped organizations gain some cost savings. However, there are even more significant savings that can be accomplished by utilizing Internet Service Providers (ISPs) and an Internet Protocol Security (IPsec) offering.

The argument between a managed network, like MPLS, versus an IPsec solution has been debated over the last several years. The argument against an IPsec solution revolves around the complexity, knowledge and training involved in engineering and managing internal and perimeter security devices. In addition, if multiple circuits are required to ensure a fault-tolerant network, BGP routers are also be required. Since the traditional IPsec solution requires a perimeter deployed architecture, the hardware and administration costs and increased complexity have driven many organizations to stay with some sort of a private network for simplicity.

Many organizations believed the trade-off for a higher cost MPLS circuit would give them a fault-tolerant, high performance, simple to manage network. However, MPLS providers cannot offer true end-to-end availability since the “last mile” of the MPLS connection is a single potential point of failure. As a result, many organizations have been forced to add standby circuits for redundancy, counter to the premise of selecting MPLS in the first place.

Today, with the advent of innovative, newer higher availability technologies included with the StoneGate solutions, the complexity and cost to administer an IPsec solution have eliminated that argument. In fact, Stonesoft customers that have replaced first generation IPsec solutions report savings of as much as 50-70 percent.

Stonesoft’s patented Multi-Link technology allows multiple communication links within a single device, providing seamless VPN failover. At the same time, all circuits are shared and load balanced, enabling full utilization of all bandwidth of all circuits seamlessly. And most importantly, the cost and administration of BGP hardware can be eliminated.

While there are many considerations involved in moving from an MPLS solution, Example 2 below outlines the potential cost savings for a 10-location organization that switched from a MPLS provider. Please note that the MPLS provider pricing included managing the remote routers as part of their service.

Example 2:

Stonesoft vs. MPLS: Annual Costs for a 10-Location Implementation

	Stonesoft				MPLS[1]			
	Qty.	**Type**	**Annual Cost/Unit**	**Total**	**Qty.**	**Type**	**Annual Cost/Unit**	**Total**
HQ Internet Connection (pair)	4	T1[2]	$4,800	$19,200	2	T1	$4,800	$9.600
HQ MPLS Connection	0	NA	$0	$0	4	T1[3]	$7,800	$31,200
Remote Circuits	20	DSL/ Cable[4]	$1,200	$24,000	10	T1	$7,800	$78,000
Administration	600 hrs.	Admin	45/hr.	$27,000	NA	NA	Included	Included
Total				**$70,200**				**$118,800**

Stonesoft vs. MPLS: 4-Year Cost Comparison

	Year 1	**Year 2**	**Year 3**	**Year 4**	**Total**
Stonesoft	$70,200	$70,200	$70,200	$70,200	$280,800
Hardware[5]	$56,900				$56,900
Hardware Support	$13,782	$13,782	$13,782	$13,782	$55,128
Total	**$140,882**	**$83,982**	**$83,982**	**$83,982**	**$392,828**
MPLS	$118,800	$118,800	$118,800	$118,800	$475,200
Hardware[6]	$70,900				$70,900
Hardware Support	$16,982	$16,982	$16,982	$16,982	$67,928
Total	**$200,682**	**$135,782**	**$135,782**	**$135,782**	**$608,028**
Total Cost Savings	**$59,800**	**$51,800**	**$51,800**	**$51,800**	**$215,200**

[1] MPLS cost is based on pricing by AT&T, July 2008
[2] ISP T1 cost is calculated at $400/month
[3] MPLS bonded T1 costs are calculated at $650/month, need 4 bonded T1's for traffic through headquarters
[4] DSL/Cable ISP cost is calculated at $100/month
[5] Stonesoft hardware costs for two firewalls at the headquarters ($15,450 each) and 10 firewalls for the remote locations ($2,600 each) for a total of $56,900
[6] MPLS hardware costs for two firewalls at the headquarters ($15,450 each) and two ISP Failover appliances ($20,000 each) for a total of $70,900

High Availability Considerations

Typically, the cost and complexity of providing a high availability solution multiplies when ensuring network availability. To provide a true high availability solution, there must be multiple circuits from different vendors. For example, when a redundant network is required, the cost of a network-based solution such as MPLS doubles, adding significant costs to the solution.

With an IPsec solution, utilizing separate ISPs allows an organization to fulfill that requirement. However, the complexity involved in using BGP to integrate two separate networks is time consuming, complex and expensive to set up and maintain.

Stonesoft's built-in always-on connectivity technologies eliminate the need for MPLS or BGP. Regardless of the type or number of connections needed, the company's patented Multi-Link technology ensures seamless VPN failover, dynamic server load balancing and optimized high availability. Let's say for instance that the availability of a DSL link is 99 percent, then there would be approximately seven hours of downtime per month. When two of these links are connected with Stonesoft's Multi-Link technology, the probability of both links going down at the same time is 0.01 percent. That is only four minutes of downtime per month. If four minutes is too much, organizations can add a third link and the potential downtime is only three seconds per month.

In addition to Multi-Link, Stonesoft can uniquely cluster up to 16 different devices and ISPs, so organizations can be assured constant availability without the need for expensive standby systems.

In most high availability implementations, three separate circuits are recommended. This allows for any one circuit to be down for maintenance and upgrades, while still maintaining fault-tolerant capabilities. However, with the StoneGate solutions in place, maintenance windows can be eliminated and devices managed in production with zero impact to the network.

Elimination of BGP and Load Balancer Costs

While maintaining multiple ISP routing, capabilities vary among vendors and approaches, whether manual or automated. For simplicity purposes, Stonesoft will consider an ISP load balancer device when calculating additional costs in a high availability environment. While an ISP load balancer can handle multiple ISPs, these devices are typically configured in a high availability configuration, hence dual appliances.

However, with Stonesoft's built-in Multi-link technology, organizations can eliminate the need for BGP, along with the ISP load balancer costs in high availability configurations.

Two ISPs		**Cost/Unit**	**Total Cost/Year**
Radware or F5	ISP Load Balancer	$21,000	$42,000

Conclusion

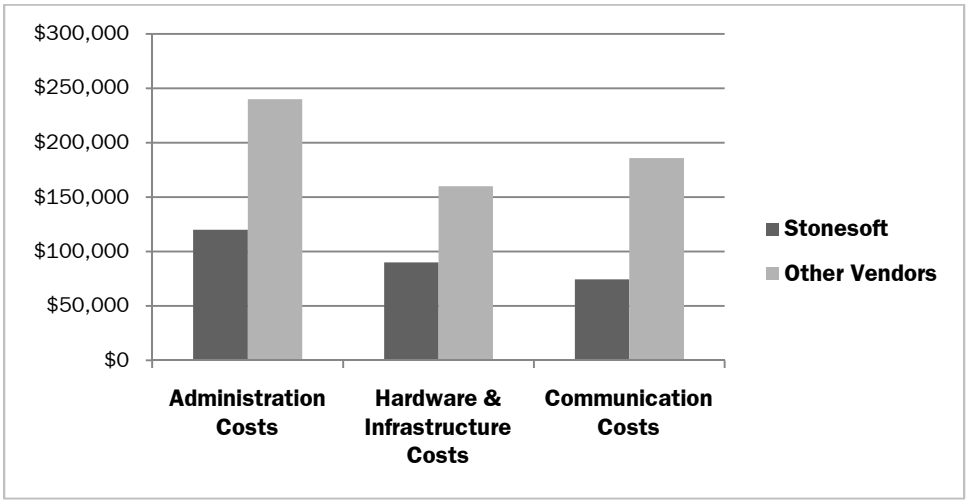
As actual analysis of real customer implementations shows in Example 3, Stonesoft has a proven track record of significantly reducing TCO by cutting administration, hardware and infrastructure, and communication costs. These three areas represent millions of dollars of unnecessary spend in network security each year. Particularly in today's economic climate, now is the time to consider new vendors, solutions and approaches that can dramatically reduce complexities and costs while optimizing network security and performance.

Example 3:

Headquarters and 30 Remote Offices, Dual Circuits, Single Firewall

4-Year Cost	Stonesoft	Other Vendors
Administration Costs (FTE = $120,000)	**$120,000**	**$240,000**
Hardware & Infrastructure Costs	**$90,000**	**$160,000**
Security appliances (HQ cluster, single node remote offices, dual ISPs)	$90,000	$90,000
Load Balancers	NA	$30,000
ISP Balancers	NA	$40,000
Communication Costs	**$74,400**[1]	**$186,000**[2]
Remote Connection	$72,000	$180,000
HQ Connection	$2,400	$6,000
Total Cost	**$284,000**	**$586,000**

[1] Dual DSL/Cable circuits in an active/active load balanced configuration at $100/month for each circuit
[2] Dual circuits in an active/passive configuration; primary is T1, and backup is DSL/Cable: $400/$100 respectively



About Stonesoft

Stonesoft Corporation (NASDAQ OMX: SFT1V) delivers proven, innovative solutions that simplify network security management for even the most complex network environments. The award-winning StoneGate Platform unifies firewall, VPN, IPS and SSL VPN, blending integrated threat management, end-to-end high availability and network optimization, into a centrally controlled system. As a result, Stonesoft provides an unparalleled level of proactive security, always-on connectivity and compliance at the lowest total cost of ownership on the market today. Founded in 1990, the company is an established leader in network security innovation with corporate headquarters in Helsinki, Finland and Americas headquarters in Atlanta, Georgia. For more information, visit www.stonesoft.com.